2019 Stakeholder Meeting

Security Standards Influence Public Safety Communication

#PSCR2019

FirstNet®

The Importance of Open Standards to FirstNet Subscribers

Mike Dolan, PhD

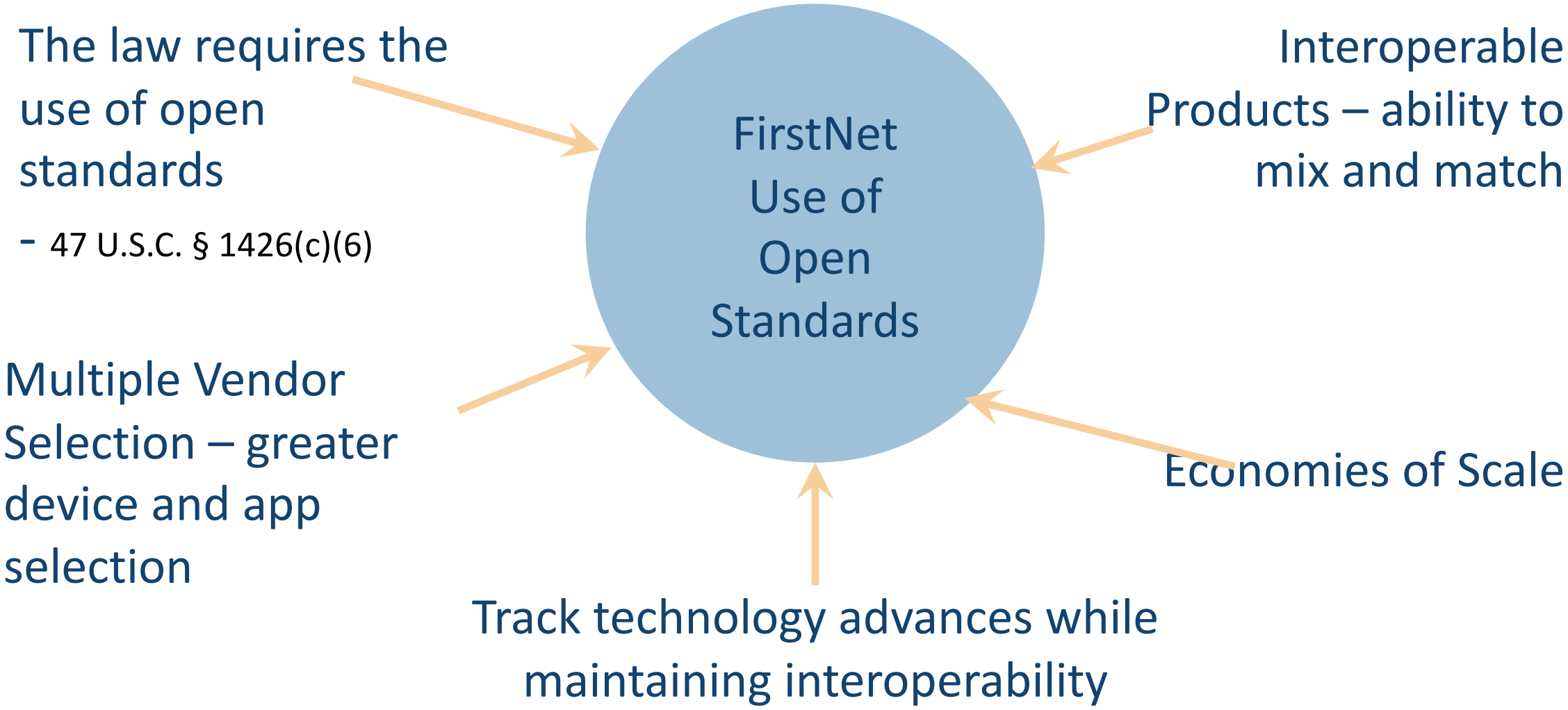
Senior Standards Engineer




DISCLAIMER

This presentation was produced by guest speaker(s) and presented at the National Institute of Standards and Technology's 2019 Public Safety Broadband Stakeholder Meeting. The contents of this presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government.

Posted with permission


The law requires the use of open standards
- 47 U.S.C. § 1426(c)(6)
Interoperable Products – ability to mix and match
FirstNet Use of Open Standards
Multiple Vendor Selection – greater device and app selection
Economies of Scale
Track technology advances while maintaining interoperability

- **Standards that support:**
- **Safety of the First Responder**
- **Access to wireless broadband communications, LTE now and a path to the future**
  - **Best technology available**
    - **Voice, high speed data, video**
  - **Interoperability with other First Responders**
    - **Including interoperability with LMR**
  - **More choice without sacrificing interoperability**
  - **Economies of scale**
    - **More features, drive prices down, and offer vendor choices for apps, devices and accessories**


FirstNet®

Topics

- **Foundational Security Standards**
- **ICAM Security Standards**
- **IoT Security Standards**

Panelist

Mike Dolan

Moderator & Sr Standards Engineer at First Responders Network Authority

Jeff Cichonski

3GPP Standards Lead
NIST/ITL

Adam Lewis

Chief Security Architect
Motorola

Bill Fisher

Security Engineer
NIST NCCoE

Foundational Standards

Jeff Cichonski, NIST/ITL

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately.

Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

***Please note, unless mentioned in reference to a NIST Publication, all information and data presented is preliminary/in-progress and subject to change**

Foundational Standards Organizations

Internet Engineering Task Force

Internet Protocols

- **TCP/IP, TLS, IPSEC**

3rd Generation Partnership Program

Cellular Systems

- **3G, LTE, VOLTE, 5G**

European Telecommunications Standards Institute

Virtualization

Standards

ICT Standards

Institute of Electrical and Electronics Engineers

802.11 - WiFi

3rd Generation Partnership Project (3GPP)

A GLOBAL INITIATIVE

Global Initiative

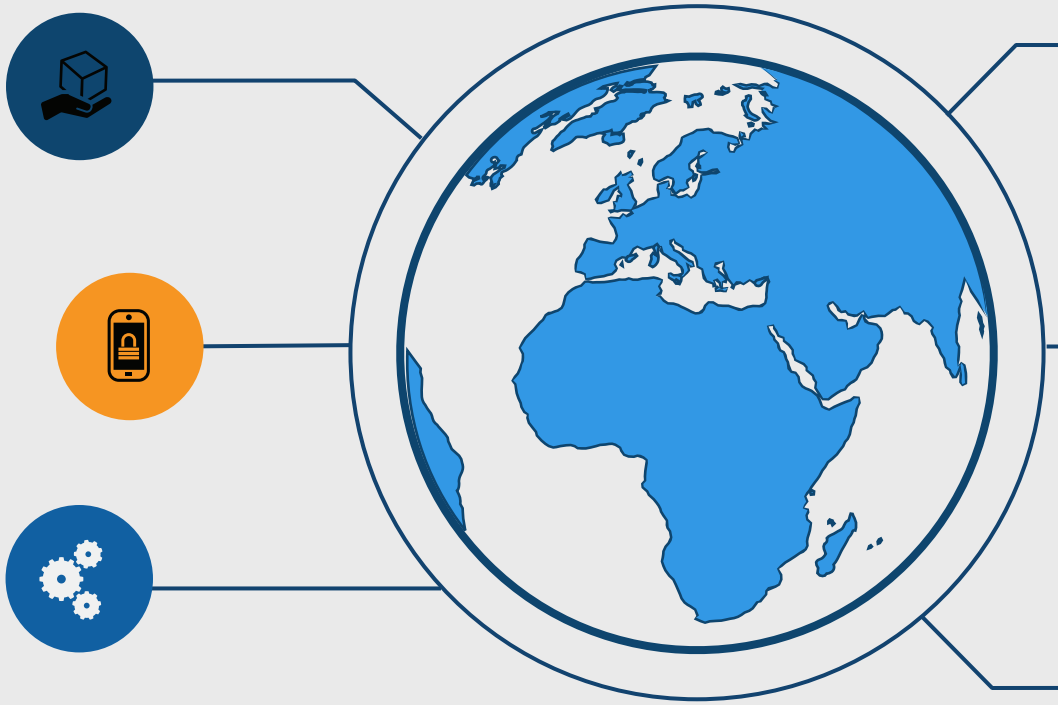
- Specs used around the world

Cellular Standards

- 3G, 4G LTE and 5G

Regional SDO's

- ATIS, ETSI, ARIB, CCSA, etc.



Technical Reports

- Studies specific topic or issue

Technical Specifications

- Presents definitive solutions

Consensus Process

- Vote = Failure

3GPP Working Groups

Radio Access Network (RAN)	Service & Systems Aspects (SA)	Core Network & Terminals (CT)
RAN 1 - Radio Layer 1 (Physical)	SA 1 - Services	CT 1 – User equipment & Core network radio protocols
RAN 2 - Radio Interface architecture and protocols	SA 2 - Architecture	CT 3 - Interworking between a 3GPP networks and external nodes or networks
RAN 3 - Radio architecture and Interface protocols	**SA 3 - Security**	CT 4 – Core network aspects
RAN 4 - Radio performance and protocol aspects	SA 4 - Codec	CT 6 – Smart card application aspects (SIMS)
RAN 5- Mobile terminal conformance testing	SA 5 - Telecom Management	
	SA 6 – Mission Critical	

NIST's Relevant Areas of Expertise

Cryptography	Advanced Encryption Standard (AES) Secure Hashing Algorithm (SHA-3) Elliptic Curve Cryptography Post Quantum Cryptography
Cybersecurity Best Practice	Framework for Improving Critical Infrastructure Cybersecurity ICT Supply Chain Risk Management Cybersecurity and Privacy for IoT Hardware Roots of Trust
Public Safety Communications	Public Safety Communications Research FirstNet 3GPP cybersecurity priorities

NIST Impacts in 3GPP SA3

- Ensured a NIST supported elliptic curve be mandatory for vendor implementation. This will be used for SUCI calculation.
- Contributed to a study analyzing drivers for 256-bit algorithms in 5G

- Supporting solutions that ensure privacy related information is never sent unprotected

- Support of specification language enabling applications to understand the security posture of their cellular connection

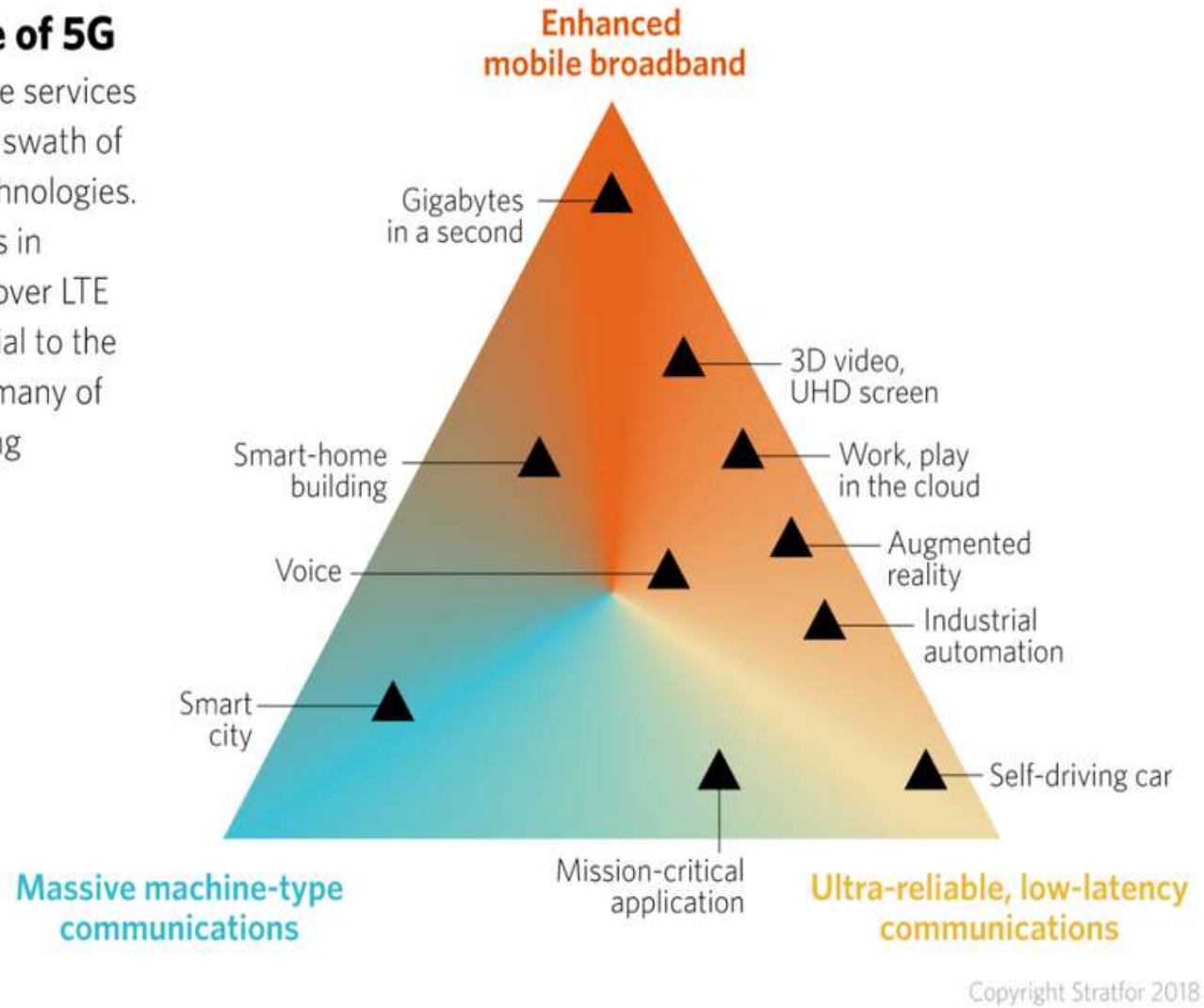
- Collaboration with the appropriate companies to ensure NIST relevant guidance and FirstNet priorities are addressed

What is 5G?

- **Enhanced Mobile Broadband**
- **Massive machine communications**
- **Ultra-reliable ultra low-latency communication**
- **…. Enhanced Security Protections?**

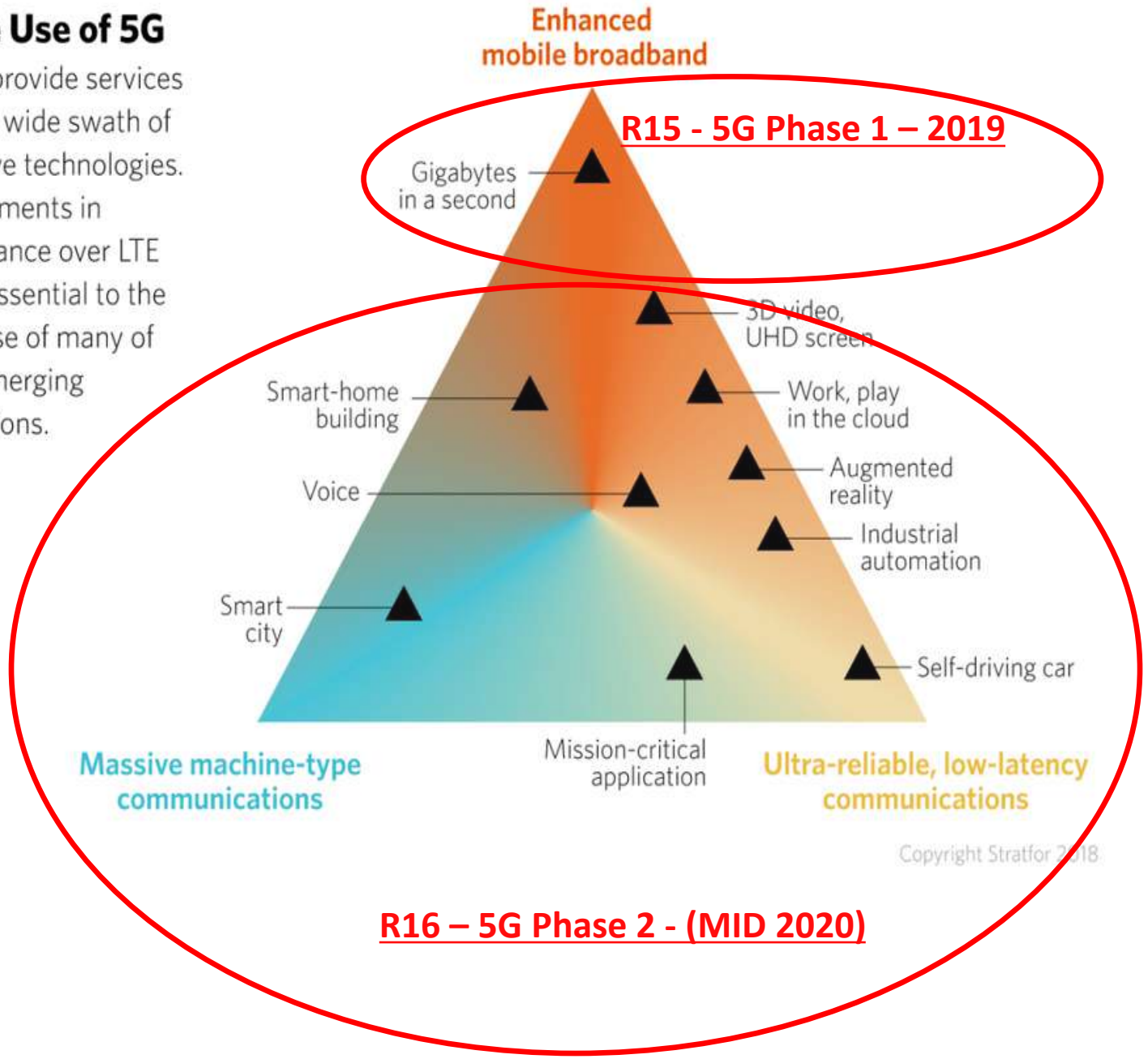
Future Use of 5G

5G will provide services across a wide swath of disruptive technologies. Improvements in performance over LTE will be essential to the future use of many of these emerging applications.

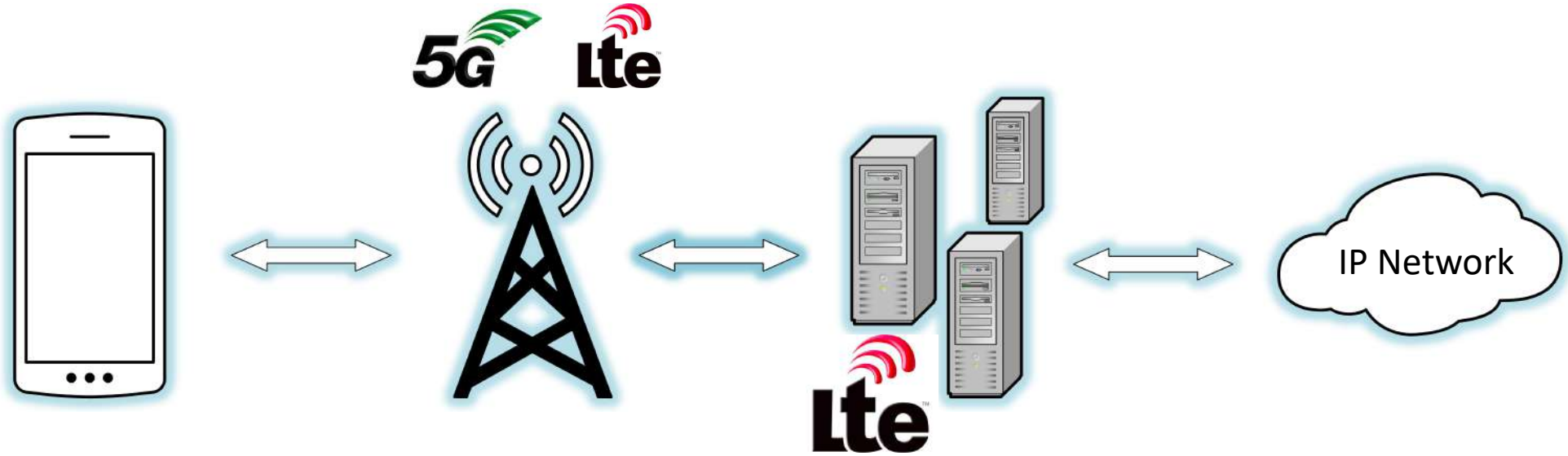


What is 5G?

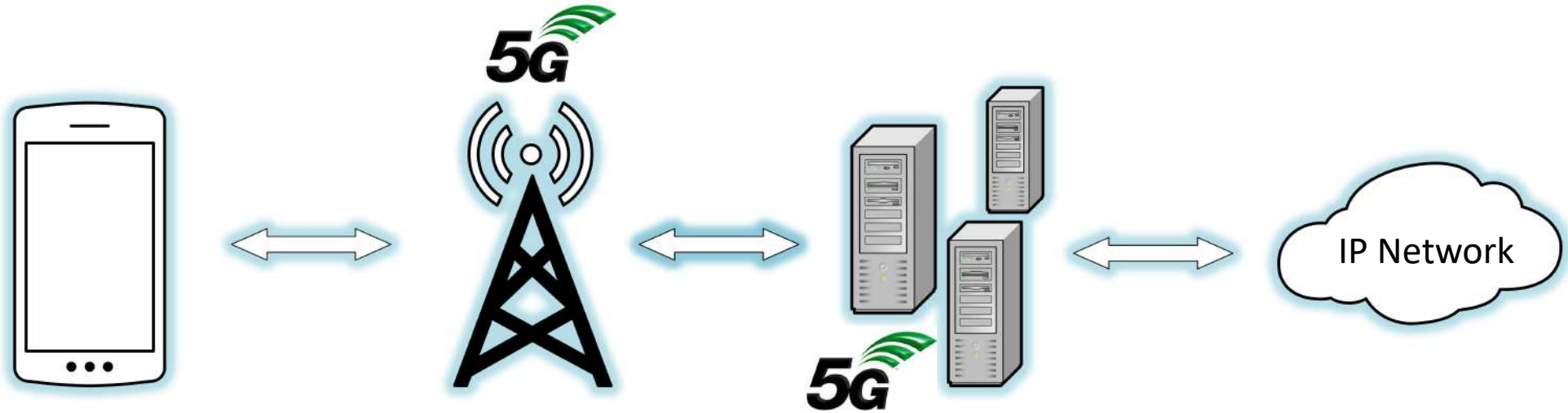
- **Enhanced Mobile Broadband**
- **Massive machine communications**
- **Ultra-reliable ultra low-latency communication**
- **…. Enhanced Security Protections?**



5G Deployments – Now



5G Deployments – Future



Contact Me

Jeff Cichonski
Information Technology Lab
National Institute of Standards and Technology

jeffreyc@nist.gov

Identity Credential & Access Management (ICAM) Standards

Adam Lewis, Motorola

DISCLAIMER

This presentation was produced by guest speaker(s) and presented at the National Institute of Standards and Technology's 2019 Public Safety Broadband Stakeholder Meeting. The contents of this presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government.

Posted with permission

Badge Credentials (The Real World)

Secure

Difficult to forge. No such thing a scalable attack that can leak all badges.

Usable

UX

Just present it wherever you want to prove your credentials. No Friction.

Interoperable

One badge. It can be used to prove your identity anywhere.

If the Badge Were Like a Password

Insecure

Badge can be copied by almost anyone and used to impersonate you. 81% of all crimes would be traced back to a compromised badge.

Unusable

Enter F0g3Ej*RykkIJ6 each time you want to present it. Go get a new badge every 30 days. Make the badge look different than the last 30 days.

Non-Interoperable

Register for a new badge everywhere you go.

If Digital Credentials were Like a Badge

Secure

Resistant to Compromise. It cannot be phished or keystroke logged or brute forced. There is no central repository to be attacked.

Usable

Digital credential used to authenticate to your home agency using frictionless biometrics. No complex passwords or 30-day rotations.

Interoperable

A single digital credential can be used to authenticate you to all digital services: home agency, public safety cloud, FirstNet, other agencies.

Open ICAM Standards

Laying the Foundation for an Identity Ecosystem

OAuth2

Delegation Authorization

OpenID Connect

Web SSO

AppAuth

Open source client library

FIDO2

Modern MFA

IETF®

OpenID

W3C®

SECURE CREDENTIALS

Standard Protocols to Look at:

- Fast ID Online (FIDO)
- Standardized by the FIDO Alliance and W3C
- Supported by Android, Major Browsers and Windows Hello
- Over 300 certified FIDO-compliant products

Leverages Innovations at the Edge:

- Commoditization of secure hardware (TEE/SE)
- Biometric Sensors

Secure:

- No storage of centralized credentials for attacker to compromise. Biometrics never leave the device. Eliminates attacks at scale. Meets requirements for CJIS and HIPAA

USABLE CREDENTIALS

Standard Protocols to Look at:
- Fast ID Online (FIDO)
- OAuth 2.0 - standardized by the IETF adoption pretty much everywhere
- AppAuth (open source library) - recommended by the IETF

Usability
- FIDO made UX a first-class citizen (biometrics)
- OAuth enables SSO across native mobile apps when implemented per IETF RFC 8252

PSFR need
- Enables open API access to PS resources, allowing ecosystem of mobile apps to emerge

INTEROPERABLE CREDENTIALS

Standard Protocols to Look at:
- OpenID Connect, Security Association Markup Language (SAML)

Interoperability
- Authentication using your strong FIDO credentials
- Access home agency network, FirstNet, Public Safety SaaS apps, NIEF, etc.

PSFR:
- Enable Inter-agency Information sharing
- Transitioning to Mobile Apps and Cloud Architectures - now is time to get the plumbing right

NIST SPECIAL PUBLICATION 1800-13

Mobile Application Single Sign-On

Improving Authentication for Public Safety First Responders

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Bill Fisher
Paul Grassi
William C. Barker
Spike E. Dog
Santos Jha
William Kim
Taylor McCorkill
Joseph Portner
Mark Russell
Sudhi Umarji

May 2019

SECOND DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/projects/use-cases/mobile-sso

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

TYING IT ALL TOGETHER

Contact Me

adam.lewis@motorolasolutions.com

@lewiada

Internet of Things (IoT) Standards

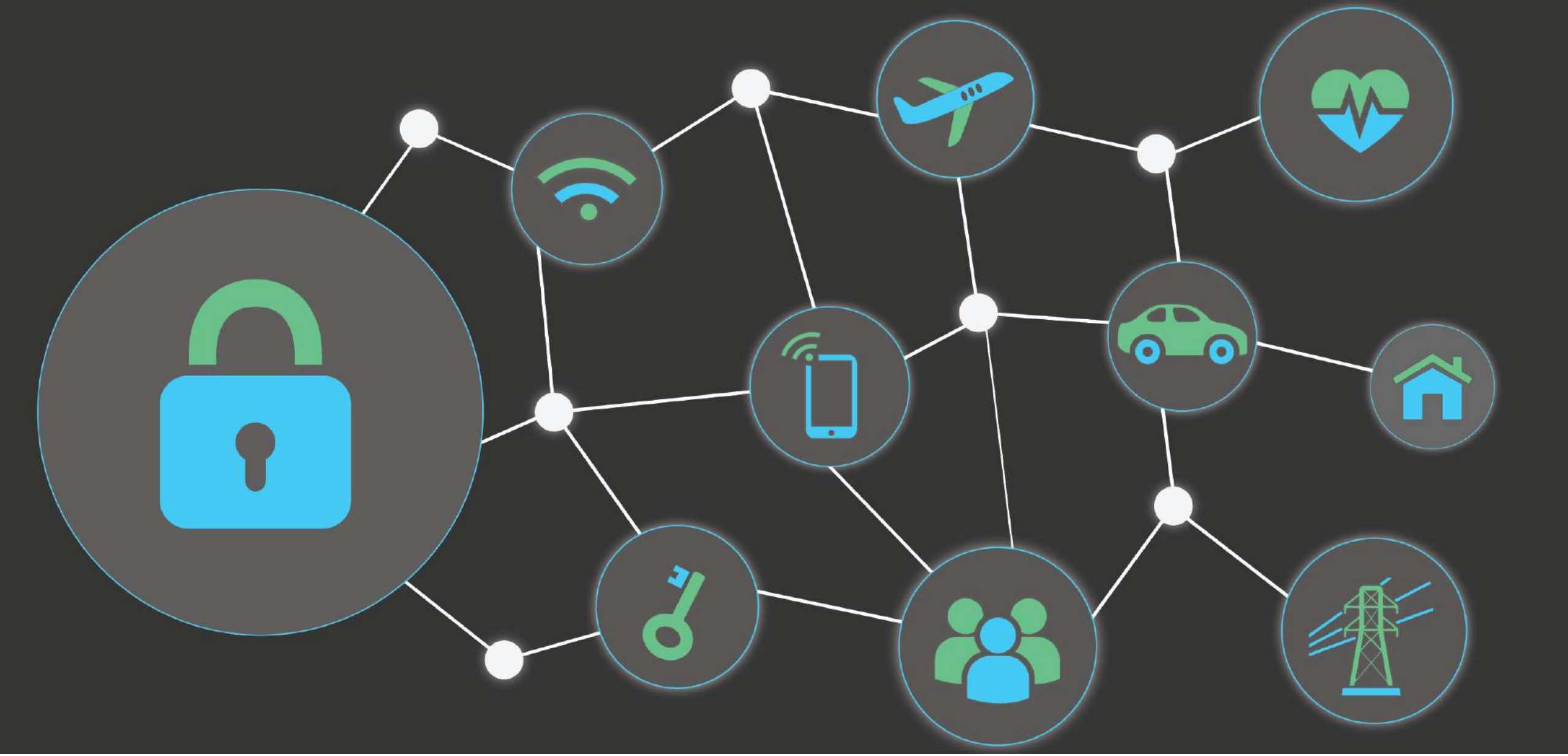
Bill Fisher, NIST/NCCoE

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately.

Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

***Please note, unless mentioned in reference to a NIST Publication, all information and data presented is preliminary/in-progress and subject to change**



Securing the World of Public Safety ‘Things”

Internet of Things - Challenges

Massive Growth

- 30 Billion Devices by 2020 - Gartner
- Over 500 billion in sales by 2020 - Gartner
- 8% of businesses are using 25% of their IoT data - Verizon

Evolving Risks

- Personal health and well being of user – firefighters health data during rescue

New Market

- **Similar to Mobile Phones of 10 years ago…**
- **Market drivers make security hard**

Internet of Things – Security Needs

Risk Based Decisions

- How devices are used
- Sensitivity of data
- Organizational risk tolerance

Security Hygiene

- Authentication
- Encryption
- Patching and updating

Interoperability

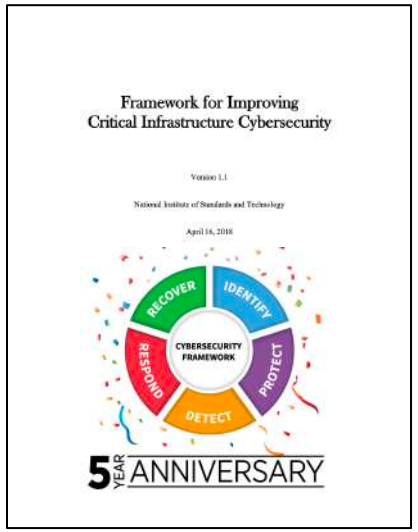
- Diverse sets of protocols
- Challenges with protocol translation

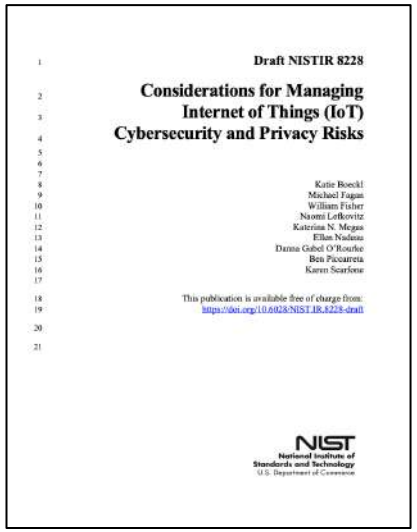
Supply Chain

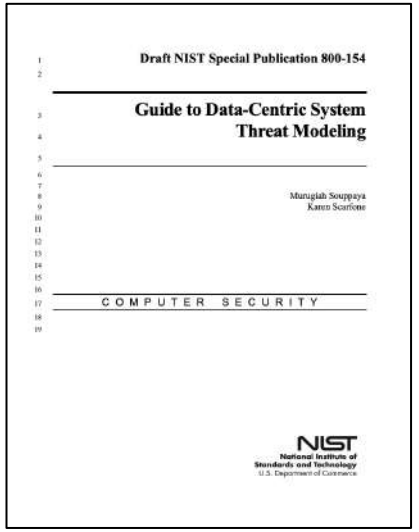
- Third-party vendor risk
- Understanding device provenance

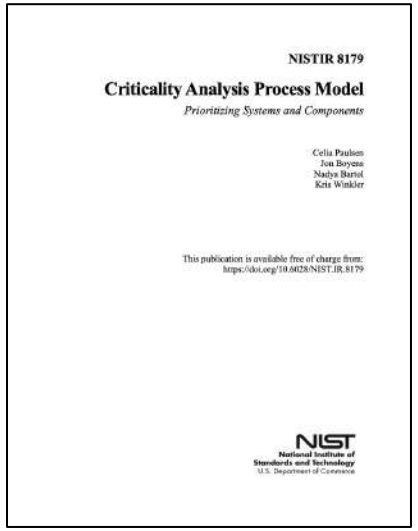
Internet of Things – Where Standards Help

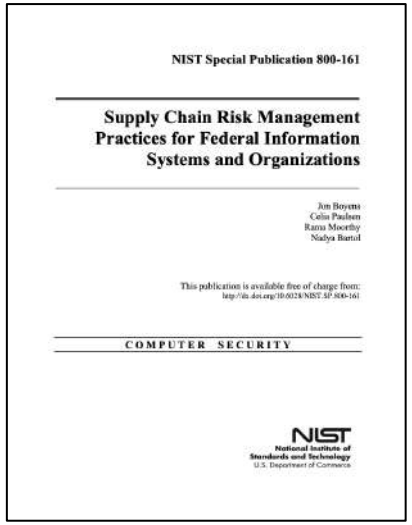
NIST Documents



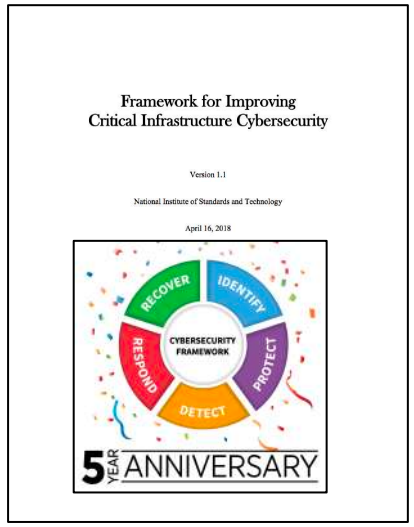








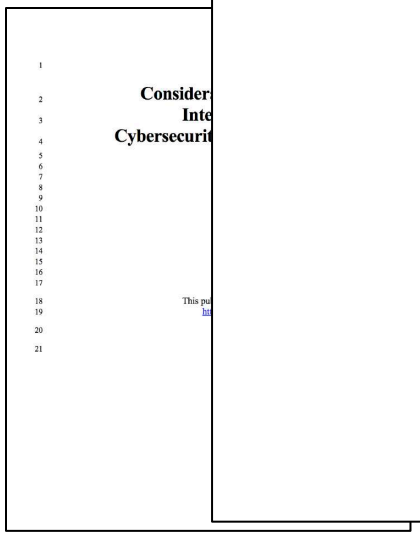
Internet of dards Help


Framework for Improving
Critical Infrastructure Cybersecurity

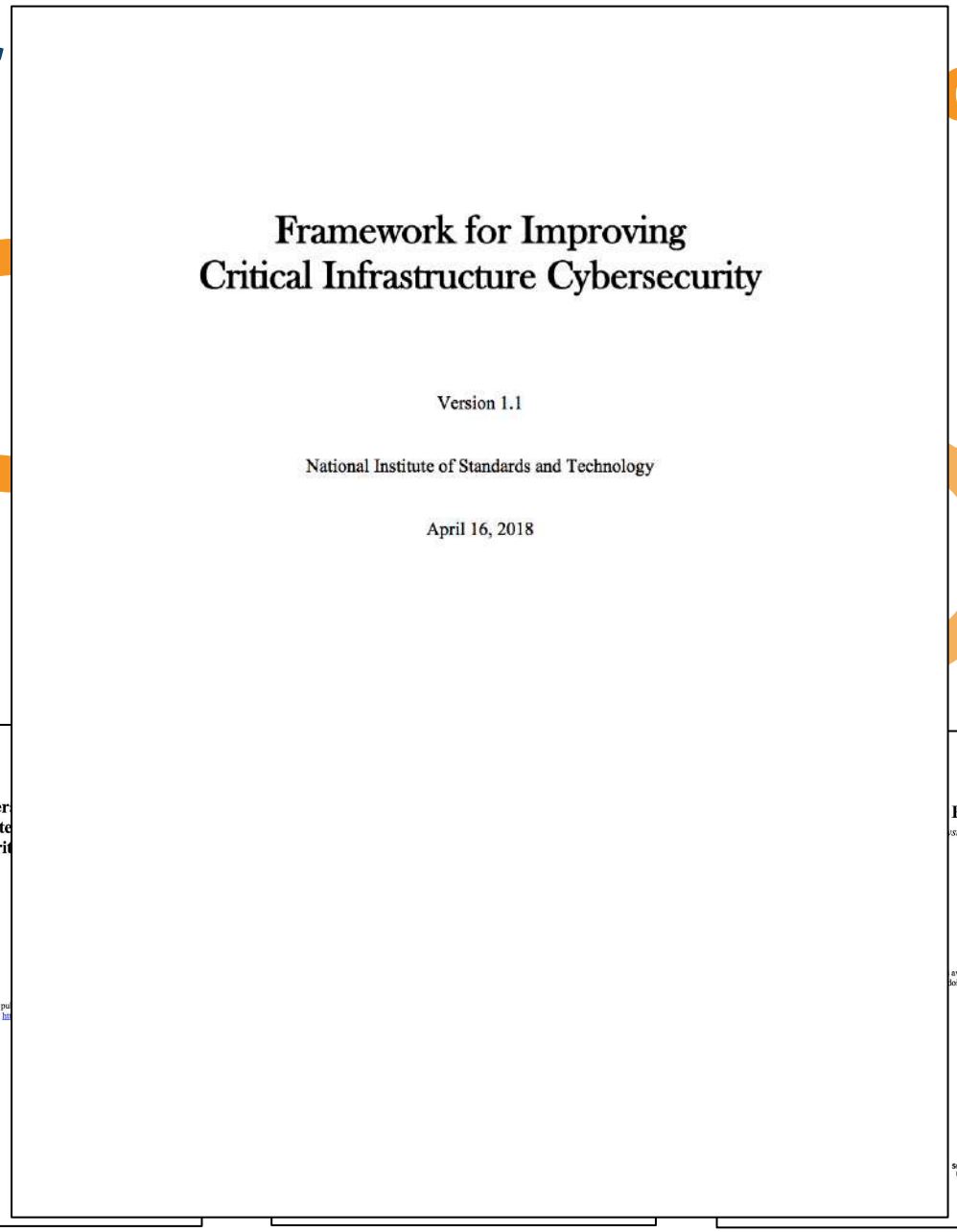
Version 1.1

National Institute of Standards and Technology

April 16, 2018


Consider
Inte
Cybersecurit

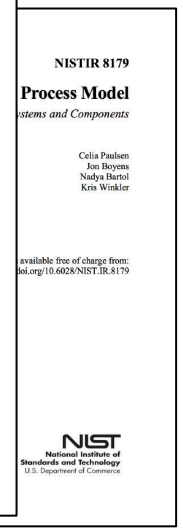
This pu


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018


NISTIR 8179

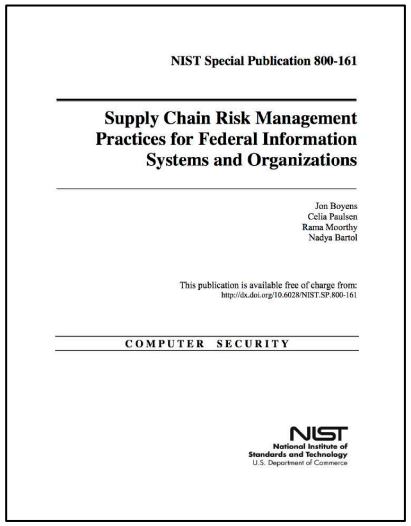
Process Model

stems and Components

Celia Paulsen
Jon Boyens
Nadya Bartol
Kris Winkler

available free of charge from:
doi.org/10.6028/NIST.IR.8179

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


NIST Special Publication 800-161

Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Jon Boyens
Celia Paulsen
Rama Moorthy
Nadya Bartol

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-161

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Internet o ndards Help

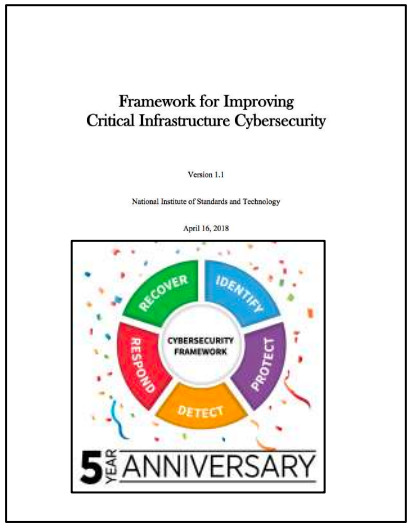
Draft NISTIR 8228

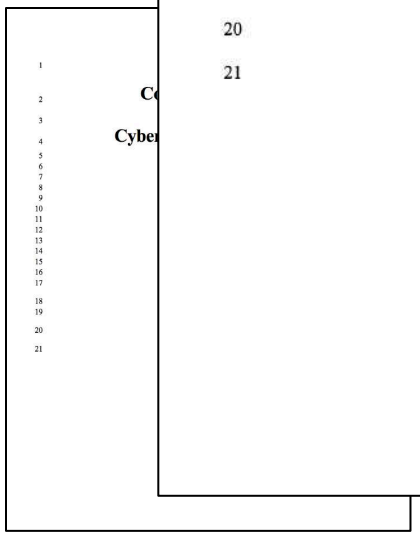
Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

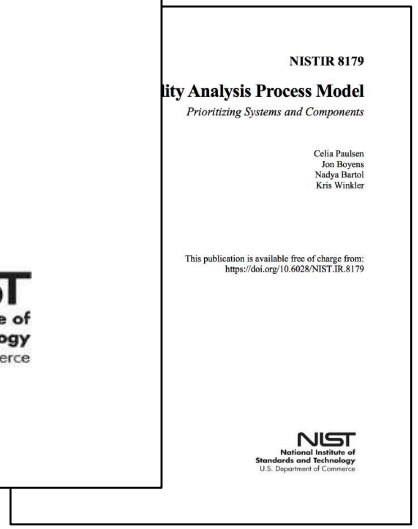
Katie Boeckl
Michael Fagan
William Fisher
Naomi Lefkovitz
Katerina N. Megas
Ellen Nadeau
Danna Gabel O'Rourke
Ben Piccarreta
Karen Scarfone

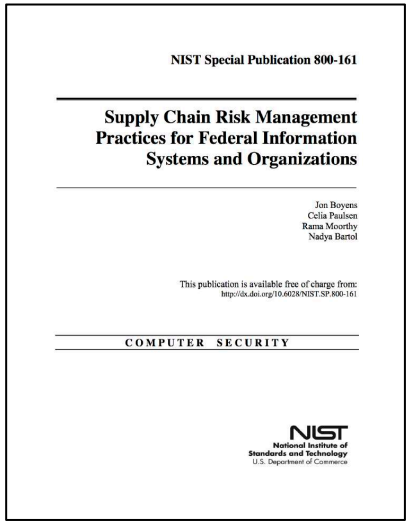
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8228-draft

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

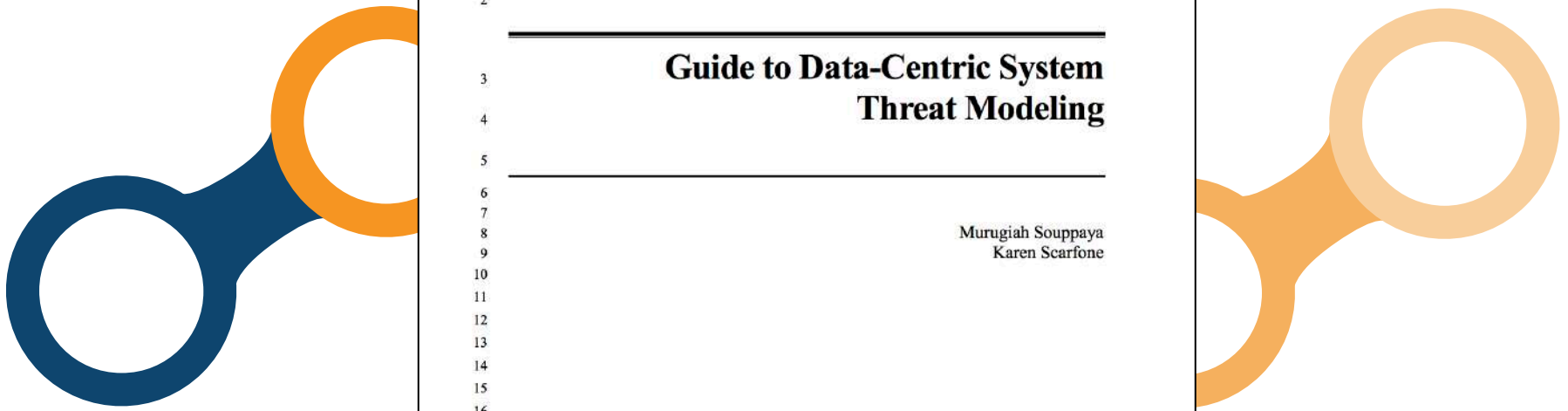


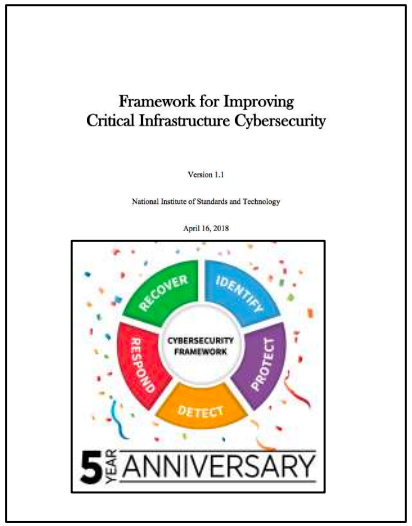


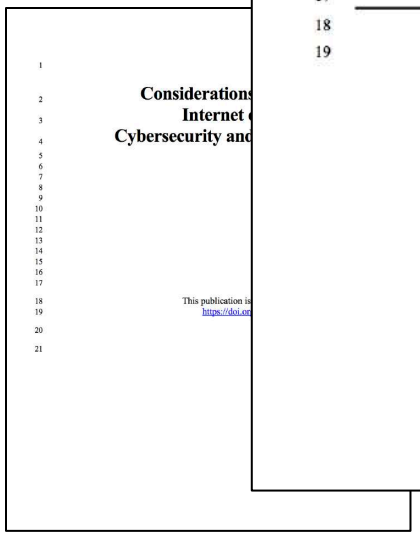


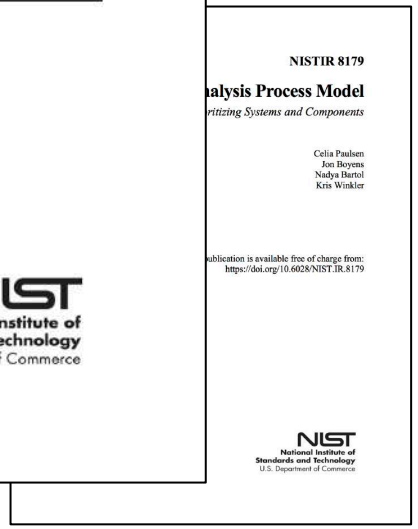


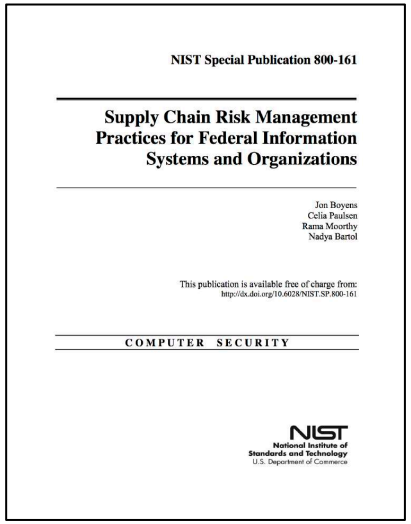
Internet of Things – Where Standards Help



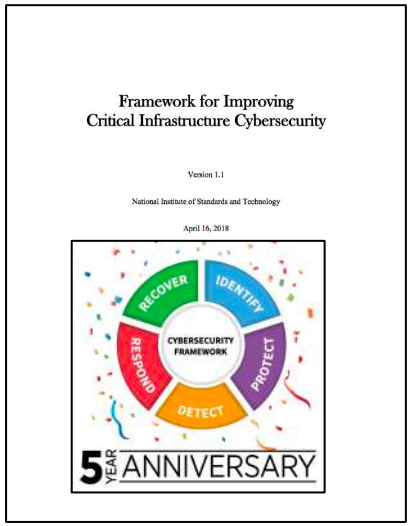








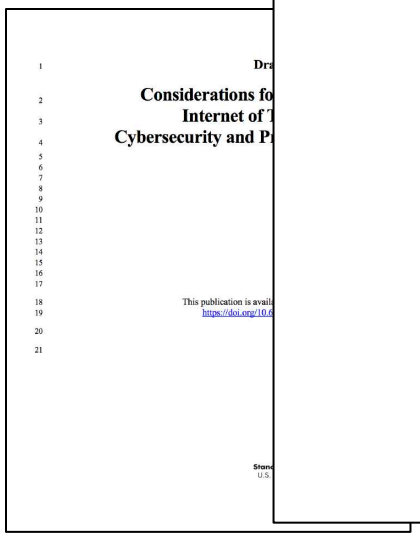
Internet of Things – Where Standards Help

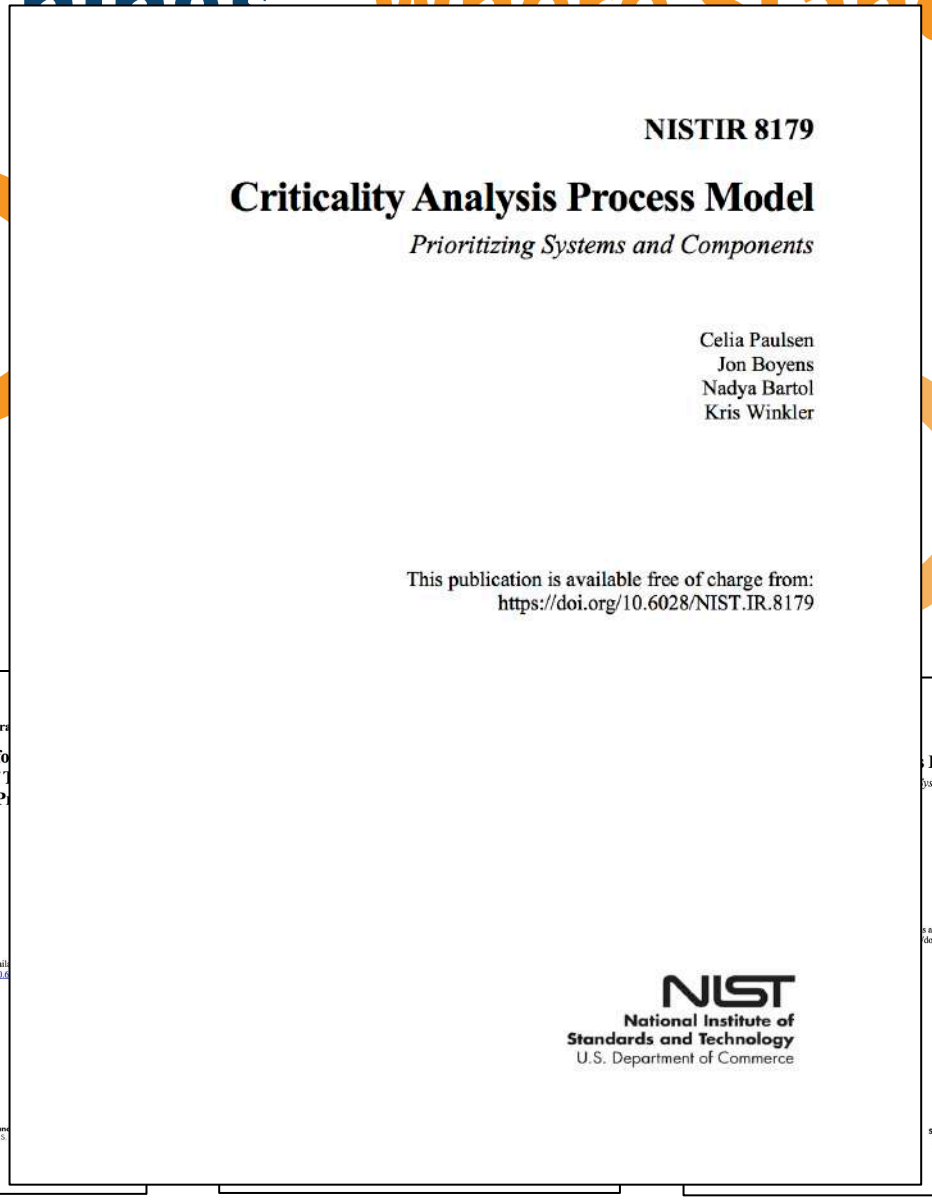

Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018


Considerations fo
Internet of
Cybersecurity and Pr


NISTIR 8179

Criticality Analysis Process Model

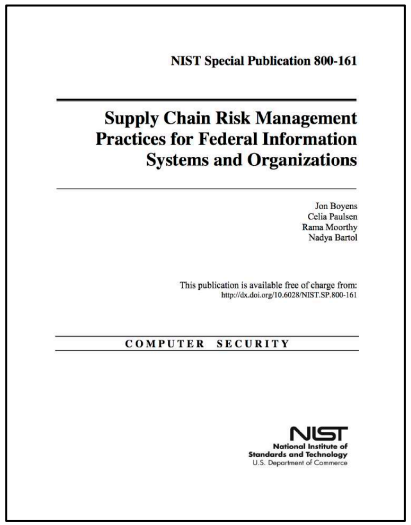
Prioritizing Systems and Components

Celia Paulsen
Jon Boyens
Nadya Bartol
Kris Winkler

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8179

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8179
Process Model
Systems and Components
Celia Paulsen
Jon Boyens
Nadya Bartol
Kris Winkler
available free of charge from:
doi.org/10.6028/NIST.IR.8179
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce


NIST Special Publication 800-161

Supply Chain Risk Management
Practices for Federal Information
Systems and Organizations

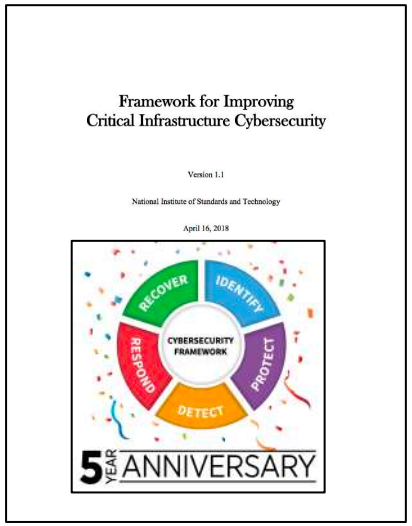
Jon Boyens
Celia Paulsen
Rama Moorthy
Nadya Bartol

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-161

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

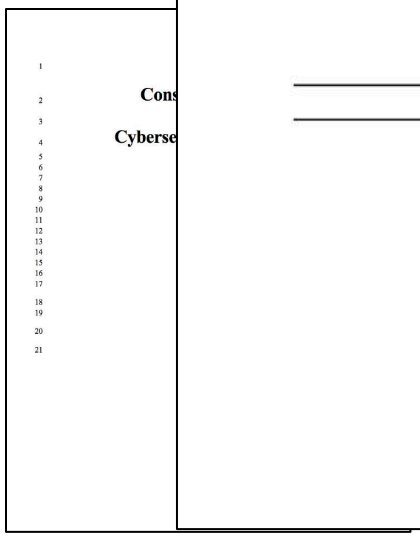
Internet of [illegible] ndards Help


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018


Cons

Cyberse

NIST Special Publication 800-161

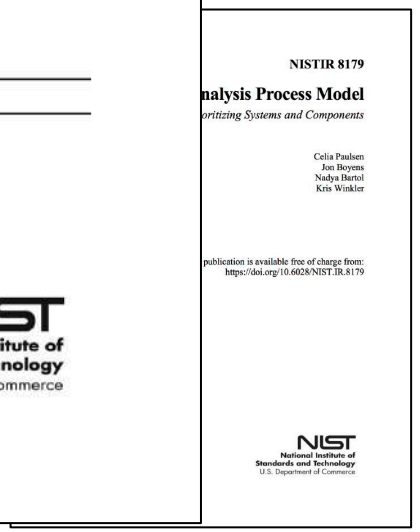
Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Jon Boyens
Celia Paulsen
Rama Moorthy
Nadya Bartol

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-161

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


NISTIR 8179

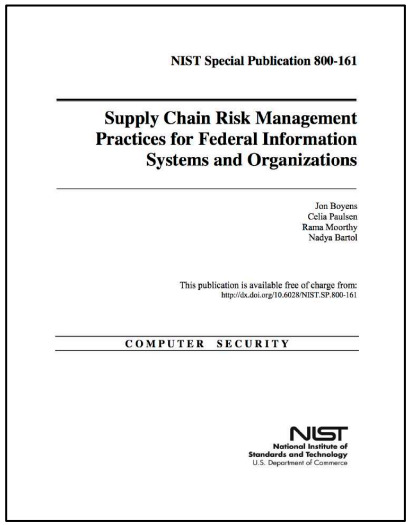
nalysis Process Model

oritizing Systems and Components

Celia Paulsen
Jon Boyens
Nadya Bartol
Kris Winkler

publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8179

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


NIST Special Publication 800-161

Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Jon Boyens
Celia Paulsen
Rama Moorthy
Nadya Bartol

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-161

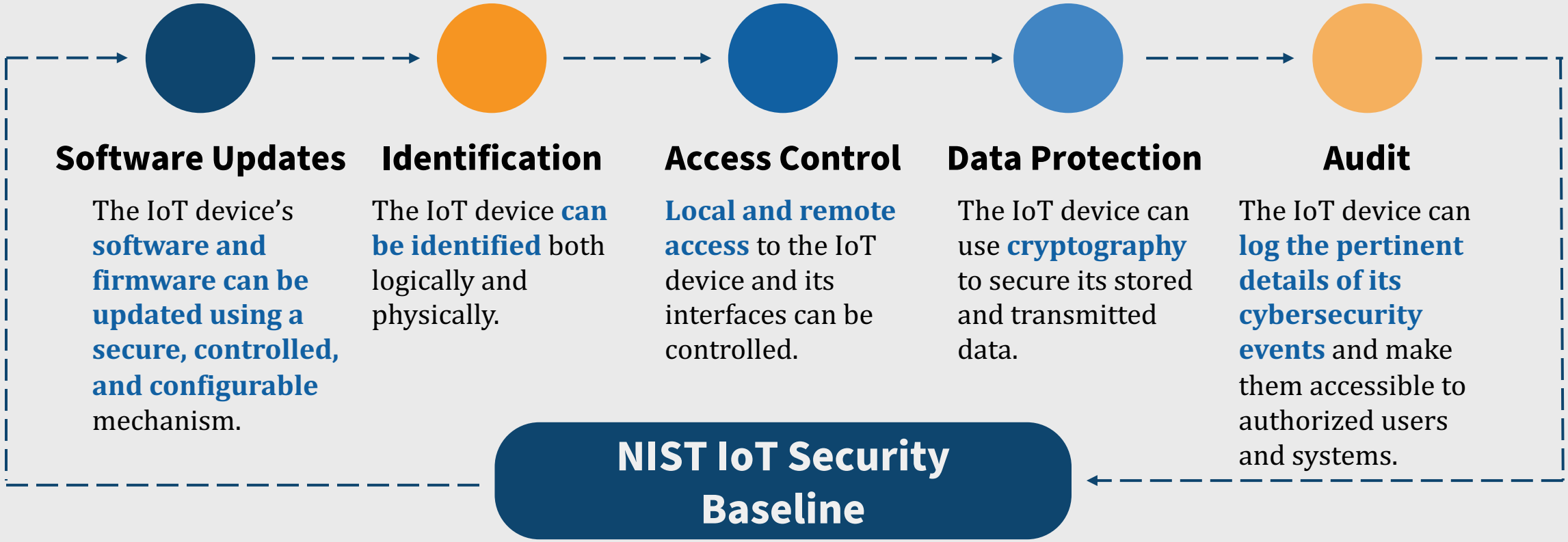
COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Internet of Things – Where Standards Help

Upcoming NIST Document – end of September

Some current considerations for the new document:



Internet of Things – Industry Standards

Manufacturer Usage Description (MUD)

- IETF Protocol - designed to be supported by network access control devices – Firewalls, routers, switches, dedicated NAC devices
- Manufacturers publish XML which identify proper device usage

ETSI TS 103 645 - Cyber Security for Consumer Internet of Things

- First standard from European Telecommunications Standards Institute
- Focuses on baseline security controls for devices

Contact Me

Bill Fisher
Security Engineer
National Cybersecurity Center of Excellence

William.Fisher@nist.gov


THANK YOU

#PSCR2019

Come back for the

Next Session

2:40 PM